Description

Authentication of key devices

The invention relates to a method as claimed in the precharacterizing clause of patent claim 1.

Such a method is described in principle in the book by W. Fumy and H.P. Rieß: Kryptographie, Entwurf und Analyse symmetrischer Kryptosysteme [Cryptography, Design and Analysis of Symmetrical Cryptosystems] R. Oldenbourg Verlag, Munich Vienna, 1988, ISBN 3-486-20868-3.

When voice or ~~, in general,~~ data are transmitted in encrypted form, both communication partners must have a joint secret, the keyword. This keyword is unknown to a potential eavesdropper or enemy. One option for this is an asymmetric encryption method, in which random numbers are interchanged between the communication partners, and are used to form joint keywords.

With this method, it is impossible to determine whether the encrypted link is being set up with the desired communication partner, or with an enemy.

Cryptographic methods may be used not only for secrecy, but also for authentication of messages. The encryption of a message using a keyword also, in principle, includes its authenticity, since an enemy cannot produce the clear text of the message without knowledge of the keyword.

In an asymmetric cryptosystem, the keyword used for encryption of a message is different to that used for decryption. Such a system, with a public and a private key, is also referred to as a public key system. The best known example of the

public key system is the so-called RSA method, whose principles are likewise described in the ~~literature~~ above-mentioned reference ~~mentioned initially~~.

At first glance, the system of key distribution is largely solved when using asymmetric cryptosystems, since the public keys can be interchanged without any problems via insecure data channels. However, this is true only provided that eavesdropping is regarded as the only risk to a communications link. However, in most cases, it is also necessary to take account of the possibility of active attacks, in addition to passive eavesdropping attempts. In this case, an active enemy introduces himself into the data link between two subscribers. Such an attack can be identified only when authentication measures are used.

The present invention is based on the need for ~~object of~~ specifying a method ~~using~~ with which it is possible to authenticate the key devices involved in data interchange.

This object is achieved according to the invention by the features specified in patent claim 1.

The invention will be described in the following text with reference to an preferred ~~exemplary~~ embodiment. The following abbreviations are used in the description that follows:

E	Encryption
D	Decryption
A, B, X	Subscribers
AD	Administrator
p	Public key
s	Secret key
pAD	Signature key, corresponds to the public key p of the administrator AD

Z	Certificate, corresponds to the public key p, to the name and further details of a subscriber X
S	Signature
S(Z)	Signature of the certificate Z

The present invention is based on a cryptomethod in which all the encryption devices are equipped with a joint public key. This public key pAD is allocated by a trustworthy entity, a so-called administrator AD. In principle, this allows any device to communicate with ~~any other, with the devices involved being~~ authenticated.

Each key device is individually assigned a certificate Z in a manner known ~~per se~~, in practice in the form of a name for ~~this~~ device. In addition, when using the public key system, the certificate Z contains the public key pX for the subscriber or user X.

According to the present invention, user groups are formed whose devices are equipped with a joint, group-specific signature key pAD. This signature key pAD is the public key pAD of the administrator AD. It may be stored in the device itself, or may be stored in the form of other storage means, ~~for example~~ such as on a smart card. ~~Such a~~ Each of the user groups has a limited number of subscribers. This limits the dissemination of the signature key pAD.

The administrator AD can produce a signature S(Z(X)) for a certificate Z(X) for a user X in a manner known ~~per se~~ in the art. In this case, the certificate Z(X) is encrypted using the secret key sAD of the administrator AD according to the relationship:

$$S(Z(X)) = E\,(Z(X),\ sAD),$$

This signature S(Z(X)) is likewise stored, in fixed or mobile form, ~~in~~ within the key device of the user X.

The ~~secret key and the public key sAD, sX and~~ (sAD, sX) and (pAD, pX) of the administrator AD and of the subscribers X are part of the public key system ~~which~~ that is implemented, for example, using the RSA algorithms.

The group-specific signature key pAD and the subscriber-specific or device-specific signature S(Z(X)) are, for example, loaded in the key device on first initialization, in ~~a refinement~~ an embodiment of the invention. In addition, the associated certificate Z(X) is stored in the key device. These data may also be distributed to the appropriate subscriber on a smart card. Personal contact with the administrator AD, or at least a secure transmission channel to ~~him~~ the administrator, is required for these procedures.

For secure communication, a link is set up between the subscribers A and B, ~~that is to say~~ (i.e.) between the associated key devices). The subscriber A transmits the certificate Z(A), and the signature S(Z(A)) to the subscriber B. The subscriber B can use the signature key pAD, ~~that is to say~~ (i.e.) the public key p of the administrator AD,) to verify the authenticity of the certificate Z(A), ~~that is to say~~ (i.e.) the authenticity of the subscriber A,) according to the relationship:

~~D(S(Z(A)), pAD) = D(E(Z(A), sAD), pAD) = Z(A)~~

The subscriber A checks the subscriber B in an analogous manner.

~~A~~ Hence a potential attacker is external to the group, has no signature S assigned by the administrator AD, and ~~can thus~~ thus can not set up a link to any subscriber in this group.

In the event of theft, the corresponding devices are excluded from the user group, so that they cannot be used by an attacker. To do this, in one possible refinement of the invention, a list of approved subscribers or key devices is stored in the key device. The identities of the possible key devices may be stored, with an appropriate security question being integrated in the process of setting up a link.

Ins. A6